

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Haruhiko KISHI, et al

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: INFORMATION VENDING APPARATUS, INFORMATION VENDING METHOD, AND PROGRAM STORAGE MEDIUM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:


<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2000-096883	March 31, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Registration No. 25,599
C. Irvin McClelland
Registration Number 21,124



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 3月31日

出願番号

Application Number:

特願2000-096883

出願人

Applicant(s):

ソニー株式会社

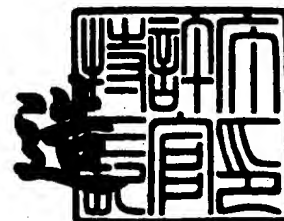


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月22日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3106198

【書類名】 特許願

【整理番号】 0000152203

【提出日】 平成12年 3月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 岸 治彦

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 栗原 章

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

特 2 0 0 0 - 0 9 6 8 8 3

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報販売装置および方法、並びにプログラム格納媒体

【特許請求の範囲】

【請求項 1】 販売する情報を蓄積する蓄積手段と、
前記情報に対応する利用条件を生成する利用条件生成手段と、
前記情報を暗号化する暗号化手段と、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成手段と、
自分自身に装着されている記録媒体を認証する認証手段と、
前記認証手段により認証された前記記録媒体に、暗号化された前記情報を前記
利用条件および前記暗号鍵と共に書き込む書き込み手段と
を含むことを特徴とする情報販売装置。

【請求項 2】 前記記録媒体に記録されている前記情報を再生する再生装置
と通信する通信手段
を更に含み、
前記認証手段は、前記通信手段が前記再生装置と通信するとき、前記再生装置
を更に認証し、
前記書き込み手段は、前記再生装置を介して、前記記録媒体に、暗号化されて
いる前記情報を前記利用条件および前記暗号鍵と共に書き込む
ことを特徴とする請求項 1 に記載の情報販売装置。

【請求項 3】 前記通信手段は、前記再生装置に一体的に設けられている前
記記録媒体に記録されている前記情報を再生する再生装置と通信し、
前記書き込み手段は、前記再生装置に一体的に設けられている前記記録媒体に
、暗号化されている前記情報を前記利用条件および前記暗号鍵と共に書き込む
ことを特徴とする請求項 2 に記載の情報販売装置。

【請求項 4】 所定の伝送路を介して送信された前記情報を受信する受信手
段
を更に含み、
前記蓄積手段は、前記受信手段が受信した前記情報を蓄積する
ことを特徴とする請求項 1 に記載の情報販売装置。

【請求項 5】 前記利用条件生成手段は、前記記録媒体に記録されている前記情報を再生する再生装置が従う前記利用条件を生成し、

前記暗号化手段は、前記再生装置が復号可能な方式で前記情報を暗号化することを特徴とする請求項 1 に記載の情報販売装置。

【請求項 6】 前記情報は、プログラム、音声、音楽、静止画像、動画像、およびテキストの少なくとも 1 つを含む

ことを特徴とする請求項 1 に記載の情報販売装置。

【請求項 7】 販売する情報を蓄積する蓄積ステップと、
前記情報に対応する利用条件を生成する利用条件生成ステップと、
前記情報を暗号化する暗号化ステップと、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、
装着されている記録媒体を認証する認証ステップと、
前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップと
を含むことを特徴とする情報販売方法。

【請求項 8】 販売する情報を蓄積する蓄積ステップと、
前記情報に対応する利用条件を生成する利用条件生成ステップと、
前記情報を暗号化する暗号化ステップと、
暗号化された前記情報を復号する暗号鍵を生成する暗号鍵生成ステップと、
装着されている記録媒体を認証する認証ステップと、
前記認証ステップの処理で認証された前記記録媒体に、暗号化された前記情報を前記利用条件および前記暗号鍵と共に書き込む書き込みステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報販売装置および方法、並びにプログラム格納媒体に関し、特に、音楽のデータなどの情報を販売する情報販売装置および方法、並びにプログラ

ム格納媒体に関する。

【 0 0 0 2 】

【従来の技術】

図 1 は、従来のデジタル情報販売システムの構成を説明する図である。デジタル情報販売装置 1 は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路 3 を介して、サーバ装置 2 から送信されたデジタル情報を受信して、その内部に記録する。デジタル情報販売装置 1 は、その内部に記録しているデジタル情報を販売するとき、購入者が所有する記録媒体 4 が装着され、装着されている記録媒体 4 にデジタル情報を記録させる。

【 0 0 0 3 】

デジタル情報販売装置 1 は、管理機能 1 1、デジタル情報蓄積機能 1 2、およびデジタル情報販売機能 1 3 を有する。管理機能 1 1 は、デジタル情報管理機能 2 1 を有し、デジタル情報蓄積機能 1 2 およびデジタル情報販売機能 1 3 を制御する。

【 0 0 0 4 】

デジタル情報蓄積機能 1 2 は、受信機能 2 2、復号機能 2 3、および記録保持機能 2 4 から構成される。受信機能 2 2 は、伝送路 3 を介して、サーバ装置 2 から送信された暗号化されているデジタル情報を受信して、復号機能 2 3 に供給する。

【 0 0 0 5 】

復号機能 2 3 は、予め、鍵を記憶し、復号機能 2 3 から供給された、暗号化されているデジタル情報を復号する。記録保持機能 2 4 は、復号機能 2 3 から供給された、復号されたデジタル情報を、デジタル情報 6 - 1 乃至 6 - 4 として記録する。

【 0 0 0 6 】

デジタル情報販売機能 1 3 は、課金機能 2 5、読み出し機能 2 6、および書き込み機能 2 7 から構成される。

【 0 0 0 7 】

課金機能 2 5 は、デジタル情報蓄積機能 1 2 に記録されているデジタル情報 6

－1乃至6－4を販売するとき、購入者から料金を徴収する。課金機能25は、更に、料金算出機能31、明細印字機能32、および料金回収機能33から構成される。

【0008】

料金算出機能31は、販売するデジタル情報6－1乃至6－4の価格を算出する。明細印字機能32は、デジタル情報6－1乃至6－4を販売するとき、領収書に販売価格などを印刷して出力する。

【0009】

料金回収機能33は、購入者により挿入された代金に対応する貨幣から、販売するデジタル情報6－1乃至6－4の価格に対応する料金を回収する。

【0010】

読み出し機能26は、販売するデジタル情報6－1乃至6－4の価格に対応する料金が支払われたとき、購入者の選択に基づいて、デジタル情報蓄積機能12が蓄積しているデジタル情報6－1乃至6－4のいずれかを読み出して、読み出したデジタル情報6－1乃至6－4のいずれかを書き込み機能27に供給する。

【0011】

書き込み機能27は、読み出し機能26から供給されたデジタル情報6－1乃至6－4のいずれかを、装着されている記録媒体4に書き込む。

【0012】

以下、デジタル情報6－1乃至6－4を個々に区別する必要がないとき、単に、デジタル情報6と称する。

【0013】

サーバ装置2は、予め定めた時刻（例えば、毎日の午前0時）に、予め記録しているデジタル情報5－1乃至5－(n+1)の中からデジタル情報販売装置1に送信するものを選択して、選択したデジタル情報5－1乃至5－(n+1)のいずれかを、伝送路3を介して、デジタル情報販売装置1に送信する。

【0014】

サーバ装置2は、管理機能51、デジタル情報集中蓄積機能52、およびデジタル情報配信サーバ機能53を有する。管理機能51は、デジタル情報管理機能

71を有し、デジタル情報集中蓄積機能52およびデジタル情報配信サーバ機能53を制御する。

【0015】

デジタル情報集中蓄積機能52は、デジタル情報販売装置1に送信するためのデジタル情報5-1乃至5-(n+1)を蓄積する。

【0016】

デジタル情報配信サーバ機能53は、デジタル情報集中蓄積機能52から蓄積されているデジタル情報5-1乃至5-(n+1)を読み出して、暗号化して、伝送路3を介して、デジタル情報販売装置1に送信する。デジタル情報配信サーバ機能53は、読み出し機能72、暗号化機能73、および送信機能74を有する。

【0017】

読み出し機能72は、デジタル情報集中蓄積機能52から蓄積されているデジタル情報5-1乃至5-(n+1)のいずれかを読み出して、暗号化機能73に供給する。暗号化機能73は、読み出し機能72から供給されたデジタル情報5-1乃至5-(n+1)のいずれかを、DES (Data Encryption Standard) などの方式で暗号化して、送信機能74に供給する。送信機能74は、暗号化されたデジタル情報5-1乃至5-(n+1)のいずれかを、伝送路3を介して、デジタル情報販売装置1に送信する。

【0018】

以下、デジタル情報5-1乃至5-(n+1)を個々に区別する必要がないとき、単にデジタル情報5と称する。

【0019】

【発明が解決しようとする課題】

しかしながら、記録媒体4には、不正なコピーまたは再生など、本来許可されていない利用を防止する機能が無く、また、デジタル情報6に対応する利用条件等も記録媒体4に記録されないので、販売されたデジタル情報について、不正な利用を防止することができないという問題点があった。

【0020】

本発明はこのような状況に鑑みてなされたものであり、販売した情報の不正な利用の防止ができるようにすることを目的とする。

【 0 0 2 1 】

【課題を解決するための手段】

請求項 1 に記載の情報販売装置は、販売する情報を蓄積する蓄積手段と、情報に対応する利用条件を生成する利用条件生成手段と、情報を暗号化する暗号化手段と、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成手段と、自分自身に装着されている記録媒体を認証する認証手段と、認証手段により認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込み手段とを含むことを特徴とする。

【 0 0 2 2 】

情報販売装置は、記録媒体に記録されている情報を再生する再生装置と通信する通信手段を更に設け、認証手段が、通信手段が再生装置と通信するとき、再生装置を更に認証し、書き込み手段が、再生装置を介して、記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

【 0 0 2 3 】

通信手段は、再生装置に一体的に設けられている記録媒体に記録されている情報を再生する再生装置と通信し、書き込み手段は、再生装置に一体的に設けられている記録媒体に、暗号化されている情報を利用条件および暗号鍵と共に書き込むようにすることができる。

【 0 0 2 4 】

情報販売装置は、所定の伝送路を介して送信された情報を受信する受信手段を更に設け、蓄積手段が、受信手段が受信した情報を蓄積するようにすることができる。

【 0 0 2 5 】

利用条件生成手段は、記録媒体に記録されている情報を再生する再生装置が従う利用条件を生成し、暗号化手段は、再生装置が復号可能な方式で情報を暗号化するようにすることができる。

【 0 0 2 6 】

情報は、プログラム、音声、音楽、静止画像、動画像、およびテキストの少なくとも1つを含むようにすることができる。

【0027】

請求項7に記載の情報販売方法は、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【0028】

請求項8に記載のプログラム格納媒体のプログラムは、販売する情報を蓄積する蓄積ステップと、情報に対応する利用条件を生成する利用条件生成ステップと、情報を暗号化する暗号化ステップと、暗号化された情報を復号する暗号鍵を生成する暗号鍵生成ステップと、装着されている記録媒体を認証する認証ステップと、認証ステップの処理で認証された記録媒体に、暗号化された情報を利用条件および暗号鍵と共に書き込む書き込みステップとを含むことを特徴とする。

【0029】

請求項1に記載の情報販売装置、請求項7に記載の情報販売方法、および請求項8に記載のプログラム格納媒体においては、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれる。

【0030】

【発明の実施の形態】

図2は、本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。デジタル情報販売装置101は、販売店（いわゆる、コンビニエンスストアなど）の店頭などに設置され、伝送路3を介して、サーバ装置2から送信されたデジタル情報（プログラム、またはテキスト、楽音を含む音楽、音声、若しくは静止画像、動画像のデータなど）を受信して、その内部に記録する。

【0031】

デジタル情報販売装置101は、例えば、音楽データであるデジタル情報を販売する場合、SDMI (Secure Digital Music Initiative) の規格に準拠して、デジタル情報に対応する利用条件を生成すると共に暗号鍵（以下、デジタル情報鍵と称する）を生成して、デジタル情報をデジタル情報鍵で復号できるように暗号化して、デジタル情報を利用条件およびデジタル情報鍵と共に、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給する。

【0032】

デジタル情報販売装置101は、DESなどの共通鍵暗号方式で、デジタル情報を暗号化するとき、デジタル情報鍵でデジタル情報を暗号化する。デジタル情報販売装置101は、RSA (Rivest-Shamir-Adleman) などの公開鍵暗号方式で、デジタル情報を暗号化するとき、秘密鍵でデジタル情報を暗号化して、公開鍵をデジタル情報鍵として、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給する。

【0033】

例えば、音楽データであるデジタル情報を利用する場合、ライセンス管理機能付デジタル情報再生装置103-1および103-2、パーソナルコンピュータ104、並びに携帯端末装置105は、SDMIの規格に準拠したソフトウェアモジュールであるLCM (Licensed Compliant Module) を有し、デジタル情報に対応する利用条件に基づいて、デジタル情報の、例えば、いわゆる、チェックイン、チェックアウト、コピー、または移動などを許可するか、または禁止する。

【0034】

ライセンス管理機能付記録媒体102-1および102-2は、デジタル情報に対応する利用条件に基づいて、記録しているデジタル情報の利用を管理する（例えば、読み出しを許可または禁止する）。

【0035】

伝送路3は、有線または無線の通信路であり、例えば、専用線、LAN (Local A

rea Network)、ISDN (Integrated Services Digital Network)、xDSL (x Digital Subscriber Line)、電話回線、PHS (Personal Handyphone System) 回線、携帯電話回線、WLL (Wireless Local Loop) 回線、通信衛星回線、または放送衛星回線などである。

【 0 0 3 6 】

デジタル情報販売装置 1 0 1 は、その内部に記録しているデジタル情報 6 を購入するために、購入者が所有するライセンス管理機能付記録媒体 1 0 2 - 1 が装置着部 1 1 1 に装着されたとき、ライセンス管理機能付記録媒体 1 0 2 - 1 との相互認証の処理を実行する。デジタル情報販売装置 1 0 1 は、デジタル情報 6 に対応する利用条件を生成するとともに、デジタル情報 6 を暗号化して、デジタル情報 6 を復号するデジタル情報鍵を生成する。

【 0 0 3 7 】

デジタル情報販売装置 1 0 1 は、認証されたライセンス管理機能付記録媒体 1 0 2 - 1 に暗号化されているデジタル情報 6 を、利用条件およびデジタル情報鍵と共に記録させる。

【 0 0 3 8 】

デジタル情報販売装置 1 0 1 によりデジタル情報 6 が記録されたライセンス管理機能付記録媒体 1 0 2 - 1 は、例えば、ライセンス管理機能付デジタル情報再生機能 1 1 4 を有する、例えば、PDA (Personal Digital Assistant)、または携帯電話機などの携帯端末装置 1 0 5 に装着される。携帯端末装置 1 0 5 のライセンス管理機能付デジタル情報再生機能 1 1 4 は、ライセンス管理機能付記録媒体 1 0 2 - 1 に記録されたデジタル情報 6 を読み出して、そのデジタル情報 6 に対応する利用条件に基づき、読み出したデジタル情報 6 を利用することができる。

【 0 0 3 9 】

購入者が所有するライセンス管理機能付記録媒体 1 0 2 - 2 が装着されているライセンス管理機能付デジタル情報再生装置 1 0 3 - 1 のインターフェース 1 1 3 - 1 は、例えば、インターフェース 1 1 3 - 1 およびインターフェース 1 1 2 の通信方式に対応するケーブル等を介して、デジタル情報販売装置 1 0 1 のイン

ターフェース 112 と接続される。デジタル情報販売装置 101 は、ライセンス管理機能付デジタル情報再生装置 103-1 が接続されたとき、ライセンス管理機能付デジタル情報再生装置 103-1 との相互認証の処理を実行する。

【0040】

なお、ライセンス管理機能付デジタル情報再生装置 103-1 は、ライセンス管理機能付記録媒体 102-2 が装着されたとき、ライセンス管理機能付記録媒体 102-2 との相互認証の処理を実行する。

【0041】

デジタル情報販売装置 101 は、認証されたライセンス管理機能付デジタル情報再生装置 103-1 に装着されているライセンス管理機能付記録媒体 102-2 に、ライセンス管理機能付デジタル情報再生装置 103-1 を介して、デジタル情報 6 を利用条件およびデジタル情報鍵と共に記録させる。

【0042】

また、ライセンス管理機能付デジタル情報再生装置 103-1 は、その内部に一体的に設けられた記憶部に、デジタル情報販売装置 101 から供給されたデジタル情報 6 を、利用条件およびデジタル情報鍵と共に記憶させるようにしてもよい。

【0043】

デジタル情報販売装置 101 によりデジタル情報 6 が記録されたライセンス管理機能付記録媒体 102-2 は、例えば、インターフェース 113-2 およびインターフェース 114 を介して、パーソナルコンピュータ 104 に接続されているライセンス管理機能付デジタル情報再生装置 103-2 に装着される。ライセンス管理機能付デジタル情報再生装置 103-2 は、そのデジタル情報 6 に対応する利用条件に基づき、ライセンス管理機能付記録媒体 102-2 に記録されたデジタル情報 6 を読み出して、読み出したデジタル情報 6 を利用することができる。

【0044】

ライセンス管理機能付記録媒体 102-1 または 102-2 は、例えば、フラッシュメモリなどの半導体メモリ、フロッピーディスクなどの磁気ディスク、コ

ンパクトディスク（商標）などの光ディスク、またはミニディスク（商標）などの光磁気ディスクなどで構成される。

【 0 0 4 5 】

また、パーソナルコンピュータ 1 0 4 は、そのデジタル情報 6 に対応する利用条件に基づき、ライセンス管理機能付デジタル情報再生装置 1 0 3 - 2 を介して、ライセンス管理機能付記録媒体 1 0 2 - 2 に記録されたデジタル情報 6 を読み出して、読み出したデジタル情報 6 を利用することができる。

【 0 0 4 6 】

なお、インターフェース 1 1 2、インターフェース 1 1 3 - 1 および 1 1 3 - 2、並びにインターフェース 1 1 4 は、USB (Universal Serial Bus)、IEEE (Institute of Electrical and Electronics Engineers) 1394、若しくは SCSI (Small Computer System Interface) などの有線の通信方式、または IrDA (Infrared Data Association) が定める赤外線通信、若しくは Bluetooth などの無線の通信方式を利用することができる。

【 0 0 4 7 】

図 3 は、デジタル情報販売装置 1 0 1 の構成の例を説明する図である。CPU (Central Processing Unit) 1 2 1 は、各種アプリケーションプログラムや、OS (Operating System) などを実際に実行する。ROM (Read-only Memory) 1 2 2 は、一般的には、CPU 1 2 1 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 1 2 3 は、CPU 1 2 1 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【 0 0 4 8 】

入力部 1 2 5 は、表示部 1 2 6 上に設けられたタッチパッド、または入力キーなどから構成され、CPU 1 2 1 に各種の指令を入力するとき、購入者により操作される。表示部 1 2 6 は、液晶表示装置または CRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。音声再生部 1 2 7 は、例えば、CPU 1 2 1 から供給されたデジタル情報 6 に含まれる音楽のデータなどを基に、音声を出力する。

【 0 0 4 9 】

通信部 1 2 8 は、伝送路 3 を介して、サーバ装置 2 から送信されたパケットに格納されているデジタル情報などのデータを CPU 1 2 1、RAM 1 2 3、または記録部 1 2 9 に出力する。

【 0 0 5 0 】

記録部 1 2 9 は、HDD (Hard Disk Drive) などで構成され、それらに CPU 1 2 1 によって実行するプログラムやデジタル情報 6 を記録または再生させる。

【 0 0 5 1 】

ドライブ 5 3 は、装着されている磁気ディスク 6 1、光ディスク 6 2、光磁気ディスク 6 3、または半導体メモリ 6 4 に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース 1 3 0、およびバス 1 2 4 を介して接続されている RAM 1 2 3 に供給する。

【 0 0 5 2 】

書き込み部 1 3 1 は、装着部 1 1 1 に装着されているライセンス管理機能付記録媒体 1 0 2 - 1 に、記録部 1 2 9 に記録されているデジタル情報 6 を書き込む。

【 0 0 5 3 】

インターフェース 1 1 2 は、所定の通信方式に対応するケーブルの一端が接続され、そのケーブルの他の一端に接続されているライセンス管理機能付デジタル情報再生装置 1 0 3 - 1 に、記録部 1 2 9 に記録されているデジタル情報 6 を送信する。

【 0 0 5 4 】

料金回収部 1 3 2 は、購入者により貨幣が投入され、貨幣が投入されたか否かを示す信号、および投入された貨幣の額に対応する信号を CPU 1 2 1 に供給する。

【 0 0 5 5 】

これらの CPU 1 2 1 乃至料金回収部 1 3 2 は、バス 1 2 4 により相互に接続されている。

【 0 0 5 6 】

図 4 は、本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。図 1 に示す場合と同様の部分には、同一の番号を付してあり、その説明は省略する。

【 0 0 5 7 】

デジタル情報販売装置 1 0 1 は、例えば、CPU 1 2 1 の所定のプログラムの実行により実現される、管理機能 2 1 1、デジタル情報蓄積機能 2 1 2、デジタル情報販売機能 2 1 3、および認証機能 2 1 4 を有する。管理機能 2 1 1 は、デジタル情報管理機能 2 2 1 を有し、例えば、購入者の操作に対応した入力部 1 2 5 の信号を基に、デジタル情報蓄積機能 2 1 2 およびデジタル情報販売機能 2 1 3 を制御する。

【 0 0 5 8 】

デジタル情報蓄積機能 2 1 2 は、受信機能 2 2 2、復号機能 2 2 3、および記録保持機能 2 2 4 から構成される。受信機能 2 2 2 は、伝送路 3 を介して、サーバ装置 2 から送信された、暗号化されているデジタル情報 5 を受信して、復号機能 2 2 3 に供給する。

【 0 0 5 9 】

復号機能 2 2 3 は、予め鍵を記憶し、復号機能 2 2 3 から供給された、暗号化されているデジタル情報 5 を復号する。記録保持機能 2 2 4 は、復号機能 2 2 3 から復号されたデジタル情報 5 を受信して、例えば、デジタル情報 6 - 1 乃至 6 - 4 として記録する。

【 0 0 6 0 】

デジタル情報販売機能 2 1 3 は、課金機能 2 2 5、読み出し機能 2 2 6、ライセンス生成機能 2 2 7、デジタル情報鍵生成機能 2 2 8、暗号化機能 2 2 9、およびライセンス付デジタル情報書き込み機能 2 3 0 から構成される。

【 0 0 6 1 】

課金機能 2 2 5 は、デジタル情報蓄積機能 2 1 2 が蓄積しているデジタル情報 6 - 1 乃至 6 - 4 を販売するとき、購入者から販売するデジタル情報 6 - 1 乃至 6 - 4 の価格に対応する料金を徴収する。課金機能 2 2 5 は、更に、料金算出機

能 231、明細印字機能 232、および料金回収機能 233 から構成される。

【0062】

料金算出機能 231 は、販売するデジタル情報 6-1 乃至 6-4 の価格を算出する。明細印字機能 232 は、デジタル情報 6-1 乃至 6-4 を販売するとき、領収書などに販売価格または販売価格に対応するバーコードなどを印刷して出力する。

【0063】

料金回収機能 233 は、料金回収部 132 の信号を基に、販売するデジタル情報 6-1 乃至 6-4 の価格に対応する料金を料金回収部 132 に回収させる。

【0064】

読み出し機能 226 は、販売するデジタル情報 6-1 乃至 6-4 の価格に対応する料金が支払われたとき、購入者の選択に対応する、デジタル情報蓄積機能 212 が蓄積しているデジタル情報 6-1 乃至 6-4 のいずれかを読み出して、読み出したデジタル情報 6-1 乃至 6-4 を暗号化機能 230 に供給する。

【0065】

ライセンス生成機能 227 は、購入者の操作に対応した入力部 125 からの信号などに基づいて、販売するデジタル情報 6-1 乃至 6-4 のそれぞれに対応する利用条件を生成して、ライセンス付デジタル情報書き込み機能 230 に供給する。

【0066】

デジタル情報鍵生成機能 228 は、販売するデジタル情報 6-1 乃至 6-4 のそれぞれに対応するデジタル情報鍵を生成して、暗号化機能 229 に供給する。

【0067】

暗号化機能 229 は、デジタル情報鍵生成機能 228 から供給されたデジタル情報鍵で復号できるように、読み出し機能 226 から供給されたデジタル情報 6-1 乃至 6-4 のそれぞれを暗号化する。暗号化機能 229 は、対応する利用条件と共に、デジタル情報 6-1 乃至 6-4 のそれぞれを暗号化するようにしてもよい。暗号化機能 229 は、暗号化したデジタル情報 6-1 乃至 6-4 を、デジタル情報鍵と共にライセンス付デジタル情報書き込み機能 230 に供給する。

【0068】

ライセンス付デジタル情報書き込み機能230は、暗号化機能229から供給されたデジタル情報6-1乃至6-4を、デジタル情報鍵および利用条件と共に、認証されたライセンス管理機能付記録媒体102-1に書き込む。また、ライセンス付デジタル情報書き込み機能230は、ライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置103-1に、暗号化されたデジタル情報6-1乃至6-4を、デジタル情報鍵および利用条件と共に書き込む。

【0069】

ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1に供給されるデジタル情報6は、図5に示すように、デジタル情報6に対応する利用条件およびデジタル情報6を復号するためのデジタル情報鍵と対応付けられている。ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1は、デジタル情報6を利用するとき、デジタル情報鍵でデジタル情報6を復号して、対応する利用条件に基づき、デジタル情報6を利用する。

【0070】

例えば、利用条件において、対応するデジタル情報6の移動は許可されているが、コピーは許可されていないとき、ライセンス管理機能付記録媒体102-1またはライセンス管理機能付デジタル情報再生装置103-1は、そのデジタル情報6を移動させるが、そのデジタル情報6を他の機器にコピーさせない。

【0071】

認証機能214は、後述する処理により、装着されたライセンス管理機能付記録媒体102-1、またはライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置103-2（接続されている）を認証する。

【0072】

なお、管理機能211、デジタル情報蓄積機能212、デジタル情報販売機能213、および認証機能214は、それぞれ、専用のハードウェアで構成するよ

うにしてもよい。

【 0 0 7 3 】

次に、購入者の所有するライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 を書き込んでデジタル情報 6 を販売するときの、デジタル情報販売装置 1 0 1 のデジタル情報 6 の販売の処理を、図 6 のフローチャートを参照して説明する。ステップ S 1 1 において、管理機能 2 1 1 は、書き込み部 1 3 1 から供給される信号を基に、ライセンス管理機能付記録媒体 1 0 2 - 1 がデジタル情報販売装置 1 0 1 の装着部 1 1 1 に装着されたか否かを判定し、ライセンス管理機能付記録媒体 1 0 2 - 1 が装着部 1 1 1 に装着されていないと判定された場合、ライセンス管理機能付記録媒体 1 0 2 - 1 が装着されるまで、ステップ S 1 1 の判定の処理を繰り返す。

【 0 0 7 4 】

ステップ S 1 1 において、ライセンス管理機能付記録媒体 1 0 2 - 1 が装着部 1 1 1 に装着されたと判定された場合、ステップ S 1 2 に進み、認証機能 2 1 4 は、装着部 1 1 1 に装着されているライセンス管理機能付記録媒体 1 0 2 - 1 との認証の処理を実行する。

【 0 0 7 5 】

図 7 は、デジタル情報販売装置 1 0 1 の認証機能 2 1 4 とライセンス管理機能付記録媒体 1 0 2 - 1 との認証の処理を説明する図である。デジタル情報販売装置 1 0 1 の認証機能 2 1 4 とライセンス管理機能付記録媒体 1 0 2 - 1 との認証の処理は、例えば、チャレンジレスポンス方式で行われる。

【 0 0 7 6 】

デジタル情報販売装置 1 0 1 は、予め、鍵 K a b および自分自身の I D を記録している。ライセンス管理機能付記録媒体 1 0 2 - 1 は、予め、鍵 K * (複数の鍵から構成される) を記録している。

【 0 0 7 7 】

デジタル情報販売装置 1 0 1 の認証機能 2 1 4 は、内部の乱数生成部で、乱数 N a および乱数 # G を生成して、I D と共に、乱数 N a および乱数 # G をライセンス管理機能付記録媒体 1 0 2 - 1 に送信する。

【 0 0 7 8 】

ライセンス管理機能付記録媒体 1 0 2 - 1 は、内部の乱数生成部で、乱数 N_b および乱数 S_b を生成する。ライセンス管理機能付記録媒体 1 0 2 - 1 は、デジタル情報販売装置 1 0 1 から送信された、デジタル情報販売装置 1 0 1 の ID、乱数 N_a 、および乱数 $\#G$ を受信する。ライセンス管理機能付記録媒体 1 0 2 - 1 の算出部は、乱数 $\#G$ に所定の関数を適用して、変数 j を生成する。

【 0 0 7 9 】

ライセンス管理機能付記録媒体 1 0 2 - 1 の算出部は、変数 j を基に、複数の鍵から構成される鍵 K^* の中から所定の鍵 $K^*_{[j]}$ を選択して、選択した鍵 $K^*_{[j]}$ を鍵として、デジタル情報販売装置 1 0 1 の ID にハッシュ関数を適用して、鍵 K_{ab} を求める。

【 0 0 8 0 】

ライセンス管理機能付記録媒体 1 0 2 - 1 の算出部は、鍵 K_{ab} を鍵として、デジタル情報販売装置 1 0 1 から受信した乱数 N_a 、生成した乱数 N_b 、およびデジタル情報販売装置 1 0 1 の ID にハッシュ関数を適用して、変数 R を算出する。

【 0 0 8 1 】

ライセンス管理機能付記録媒体 1 0 2 - 1 は、乱数 N_b 、変数 R 、変数 j 、および乱数 S_b をデジタル情報販売装置 1 0 1 に送信する。

【 0 0 8 2 】

デジタル情報販売装置 1 0 1 は、ライセンス管理機能付記録媒体 1 0 2 - 1 が送信した、乱数 N_b 、変数 R 、変数 j 、および乱数 S_b を受信する。

【 0 0 8 3 】

デジタル情報販売装置 1 0 1 の認証機能 2 1 4 は、鍵 K_{ab} を鍵として、乱数 N_a 、ライセンス管理機能付記録媒体 1 0 2 - 1 から受信した乱数 N_b 、および自分自身の ID にハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体 1 0 2 - 1 から受信した変数 R と等しいか否かを判定し、鍵 K_{ab} を鍵として、乱数 N_a 、乱数 N_b 、および ID にハッシュ関数を適用して算出された値が変数 R と等しいと判定された場合、ライセンス管理機能付記録媒体 1 0 2

ー 1 を正当であると認証する。

【0084】

鍵 K_{ab} を鍵として、乱数 N_a 、乱数 N_b 、および ID にハッシュ関数を適用して算出された値が変数 R と等くないと判定された場合、デジタル情報販売装置 101 の認証機能 214 は、ライセンス管理機能付記録媒体 102-1 が正当でないと判定し、ライセンス管理機能付記録媒体 102-1 を認証せず、処理は終了する。

【0085】

ライセンス管理機能付記録媒体 102-1 を正当であると認証された場合、デジタル情報販売装置 101 の認証機能 214 は、鍵 K_{ab} を鍵として、乱数 N_b および乱数 N_a にハッシュ関数を適用して、変数 R' を算出する。デジタル情報販売装置 101 の認証機能 214 は、鍵 K_{ab} を鍵として、乱数 S_a および乱数 S_b にハッシュ関数を適用して、一時鍵 K_s を算出する。

【0086】

デジタル情報販売装置 101 の認証機能 214 は、変数 R' および乱数 S_a をライセンス管理機能付記録媒体 102-1 に送信する。

【0087】

ライセンス管理機能付記録媒体 102-1 は、デジタル情報販売装置 101 から送信された変数 R' および乱数 S_a を受信する。

【0088】

ライセンス管理機能付記録媒体 102-1 は、鍵 K_{ab} を鍵として、乱数 N_b 、および乱数 N_a にハッシュ関数を適用して算出された値が、ライセンス管理機能付記録媒体 102-1 から受信した変数 R' と等しいか否かを判定し、鍵 K_{ab} を鍵として、乱数 N_b 、および乱数 N_a にハッシュ関数を適用して算出された値が、変数 R' と等しいと判定された場合、デジタル情報販売装置 101 を正当であると認証する。

【0089】

鍵 K_{ab} を鍵として、乱数 N_b 、および乱数 N_a にハッシュ関数を適用して算出された値が、変数 R' と等くないと判定された場合、ライセンス管理機能付記

録媒体 102-1 は、デジタル情報販売装置 101 が正当でないと判定し、デジタル情報販売装置 101 を認証せず、処理は終了する。

【0090】

デジタル情報販売装置 101 が正当であると認証された場合、ライセンス管理機能付記録媒体 102-1 は、鍵 K a b を鍵として、乱数 S a および乱数 S b にハッシュ関数を適用して、一時鍵 K s を算出する。

【0091】

このように、デジタル情報販売装置 101 とライセンス管理機能付記録媒体 102-1 とは、相互認証すると共に、相互認証されたとき、共通の一時鍵 K s を共有する。

【0092】

なお、認証の処理で利用されるハッシュ関数として、DESを利用するようにしてもよい。

【0093】

ステップ S 13 において、管理機能 211 は、ステップ S 12 の処理でライセンス管理機能付記録媒体 102-1 が認証されたか否かを判定し、ライセンス管理機能付記録媒体 102-1 が認証されたと判定された場合、ステップ S 14 に進み、デジタル情報蓄積機能 212 から供給されるデータを基に、表示部 126 に、販売可能なデジタル情報 6 の選択画面を表示させる。

【0094】

ステップ S 15 において、管理機能 211 は、購入者の操作に対応した入力部 125 からの信号を基に、販売するデジタル情報 6 が決定されたか否かを判定し、販売するデジタル情報 6 が決定されたと判定された場合、ステップ S 16 に進み、デジタル情報販売機能 213 の料金算出機能 231 に、販売するデジタル情報 6 の価格を算出させる。

【0095】

ステップ S 17 において、管理機能 211 は、デジタル情報販売機能 213 の料金回収部 132 からの信号を基に、料金回収部 132 に代金が投入されたか否かを判定し、料金回収部 132 に代金が投入されたと判定された場合、ステップ

S 1 8 に進み、料金回収部 1 3 2 に投入された代金を料金回収機能 2 3 3 に数えさせる。

【 0 0 9 6 】

ステップ S 1 9 において、管理機能 2 1 1 は、ステップ S 1 6 で算出されたデジタル情報 6 の価格、および料金回収機能 2 3 3 から供給された、料金回収部 1 3 2 に投入された代金に対応する信号を基に、投入された代金でデジタル情報 6 が販売できるか否かを判定し、投入された代金でデジタル情報 6 が販売できると判定された場合、ステップ S 2 0 に進み、読み出し機能 2 2 6 に、記録保持機能 2 2 4 から所定のデジタル情報 6 を読み出させる。ライセンス生成機能 2 2 7 は、読み出したデジタル情報 6 に対応する利用条件を生成する。デジタル情報鍵生成機能 2 2 8 は、デジタル情報 6 を復号するデジタル情報鍵を生成する。暗号化機能 2 2 9 は、例えば、DES の方式で、デジタル情報 6 を暗号化する。

【 0 0 9 7 】

ライセンス付デジタル情報書き込み機能 2 3 0 は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 を記録する。

【 0 0 9 8 】

ステップ S 2 1 において、管理機能 2 1 1 は、書き込み部 1 3 1、またはライセンス付デジタル情報書き込み機能 2 3 0 から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 が正常に記録されたと判定された場合、ステップ S 2 2 に進み、デジタル情報販売装置 1 0 1 の装着部 1 1 1 からライセンス管理機能付記録媒体 1 0 2 - 1 を排出させ、処理は終了する。

【 0 0 9 9 】

ステップ S 1 3 において、ライセンス管理機能付記録媒体 1 0 2 - 1 が認証されないと判定された場合、ライセンス管理機能付記録媒体 1 0 2 - 1 が正当ではないので、ステップ S 2 3 に進み、管理機能 2 1 1 は、表示部 1 2 6 に認証され

なかった旨を示すエラーメッセージを表示させ、処理は終了する。

【0100】

ステップS15において、販売するデジタル情報6が決定されず、処理の中止が要求されたと判定された場合、ステップS24に進み、管理機能211は、表示部126に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0101】

ステップS17において、料金回収部132に代金が投入されず、処理の中止が要求されたと判定された場合、ステップS25に進み、管理機能211は、表示部126に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0102】

ステップS19において、投入された代金でデジタル情報6が販売できないと判定された場合、ステップS26に進み、管理機能211は、表示部126に、代金が足りないので処理が中断された旨を示すメッセージを表示させ、料金回収部132に投入された代金を排出させて、処理は終了する。

【0103】

ステップS21において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されないと判定された場合、ステップS27に進み、管理機能211は、表示部126に、書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【0104】

以上のように、デジタル情報販売装置101は、ライセンス管理機能付記録媒体102-1に、デジタル情報鍵および利用条件と共に、デジタル情報6を記録させることができる。

【0105】

なお、デジタル情報販売装置101は、同様の処理で、ライセンス管理機能付記録媒体102-2が装着されているライセンス管理機能付デジタル情報再生装置103-1に、デジタル情報鍵および利用条件と共にデジタル情報6を書き込

む。

【0106】

次に、購入者の所有するライセンス管理機能付記録媒体102-1にデジタル情報6を書き込んでデジタル情報6を販売するときの、デジタル情報販売装置101のデジタル情報6の販売の他の処理を、図8のフローチャートを参照して説明する。ステップS51乃至ステップS55の処理は、図6のステップS11乃至ステップS15の処理と、それぞれ同様であるので、その説明は省略する。

【0107】

ステップS55において、販売するデジタル情報6が決定されたと判定された場合、ステップS56に進み、管理機能11は、読み出し機能226に、記録保持機能224から販売が決定されたデジタル情報6を読み出させる。ライセンス生成機能227は、読み出したデジタル情報6に対応する利用条件を生成する。デジタル情報鍵生成機能228は、デジタル情報6を復号するデジタル情報鍵を生成する。暗号化機能229は、例えば、DESの方式で、デジタル情報6を暗号化する。

【0108】

ライセンス付デジタル情報書き込み機能230は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6を記録する。

【0109】

ステップS57において、管理機能211は、書き込み部131、またはライセンス付デジタル情報書き込み機能230から供給される信号を基に、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されたか否かを判定し、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体102-1にデジタル情報6が正常に記録されたと判定された場合、ステップS58に進み、管理機能211は、デジタル情報販売機能213の料金算出機能231に、販売するデジタル情報6の価格を算出させる。

【0110】

ステップ S 5 9 において、管理機能 2 1 1 は、明細印字機能 2 3 2 に、ステップ S 5 8 の処理で算出した販売するデジタル情報 6 の価格を、数字およびバーコードなどで領収書に印刷させる。

【0 1 1 1】

ステップ S 6 0 において、管理機能 2 1 1 は、デジタル情報販売装置 1 0 1 の装着部 1 1 1 からライセンス管理機能付記録媒体 1 0 2 - 1 を排出させる。

【0 1 1 2】

ステップ S 6 1 において、管理機能 2 1 1 は、料金回収機能 2 3 3 に、販売するデジタル情報 6 の価格に対応する、支払われた料金を受け取らせ、処理は終了する。

【0 1 1 3】

ステップ S 5 3 において、ライセンス管理機能付記録媒体 1 0 2 - 1 が認証されないと判定された場合、ライセンス管理機能付記録媒体 1 0 2 - 1 が正当ではないので、ステップ S 6 2 に進み、管理機能 2 1 1 は、表示部 1 2 6 に認証されなかった旨を示すエラーメッセージを表示させ、処理は終了する。

【0 1 1 4】

ステップ S 5 5 において、販売するデジタル情報 6 が決定されず、中止が要求されたと判定された場合、ステップ S 6 3 に進み、管理機能 2 1 1 は、表示部 1 2 6 に処理が中断された旨を示すメッセージを表示させ、処理は終了する。

【0 1 1 5】

ステップ S 5 7 において、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 が正常に記録されないと判定された場合、ステップ S 6 4 に進み、管理機能 2 1 1 は、表示部 1 2 6 に書き込みが失敗した旨を示すエラーメッセージを表示させ、処理は終了する。

【0 1 1 6】

このように、デジタル情報販売装置 1 0 1 のデジタル情報 6 の販売の他の処理によっても、デジタル情報販売装置 1 0 1 は、デジタル情報鍵および利用条件と共に、ライセンス管理機能付記録媒体 1 0 2 - 1 にデジタル情報 6 を記録させることができる。

【 0 1 1 7 】

なお、ステップ S 6 1 の処理において、料金回収機能 2 3 3 が、販売するデジタル情報 6 の価格に対応する料金を受け取ると説明したが、購入者に、デジタル情報販売装置 1 0 1 が設置されている販売店の金銭の支払いをする場所で、ステップ S 5 9 の処理で印刷された、販売するデジタル情報 6 の価格を基に、料金を支払わせるようにしてもよい。

【 0 1 1 8 】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【 0 1 1 9 】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図 3 に示すように、磁気ディスク 1 6 1 (フロッピディスクを含む)、光ディスク 1 6 2 (CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク 1 6 3 (MD(Mini-Disc)を含む)、若しくは半導体メモリ 1 6 4 などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納される ROM 1 2 2 や、記録部 1 2 9 を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどの通信部 1 2 8 を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【 0 1 2 0 】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0121】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0122】

【発明の効果】

請求項1に記載の情報販売装置、請求項7に記載の情報販売方法、および請求項8に記載のプログラム格納媒体によれば、販売する情報が蓄積され、情報に対応する利用条件が生成され、情報が暗号化され、暗号化された情報を復号する暗号鍵が生成され、装着されている記録媒体が認証され、認証された記録媒体に、暗号化された情報が利用条件および暗号鍵と共に書き込まれるようにしたので、販売した情報の不正な利用の防止ができるようになる。

【図面の簡単な説明】

【図1】

従来のデジタル情報販売システムの構成を説明する図である。

【図2】

本発明に係るデジタル情報販売システムの一実施の形態を説明する図である。

【図3】

デジタル情報販売装置101の構成の例を説明する図である。

【図4】

本発明に係るデジタル情報販売システムの一実施の形態の構成を説明する図である。

【図5】

利用条件およびデジタル情報鍵が付加されたデジタル情報6を説明する図である。

【図6】

デジタル情報販売装置101のデジタル情報6の販売の処理を説明するフローチャートである。

【図7】

デジタル情報販売装置101の認証機能214とライセンス管理機能付記録媒

体 102-1 との認証の処理を説明する図である。

【図 8】

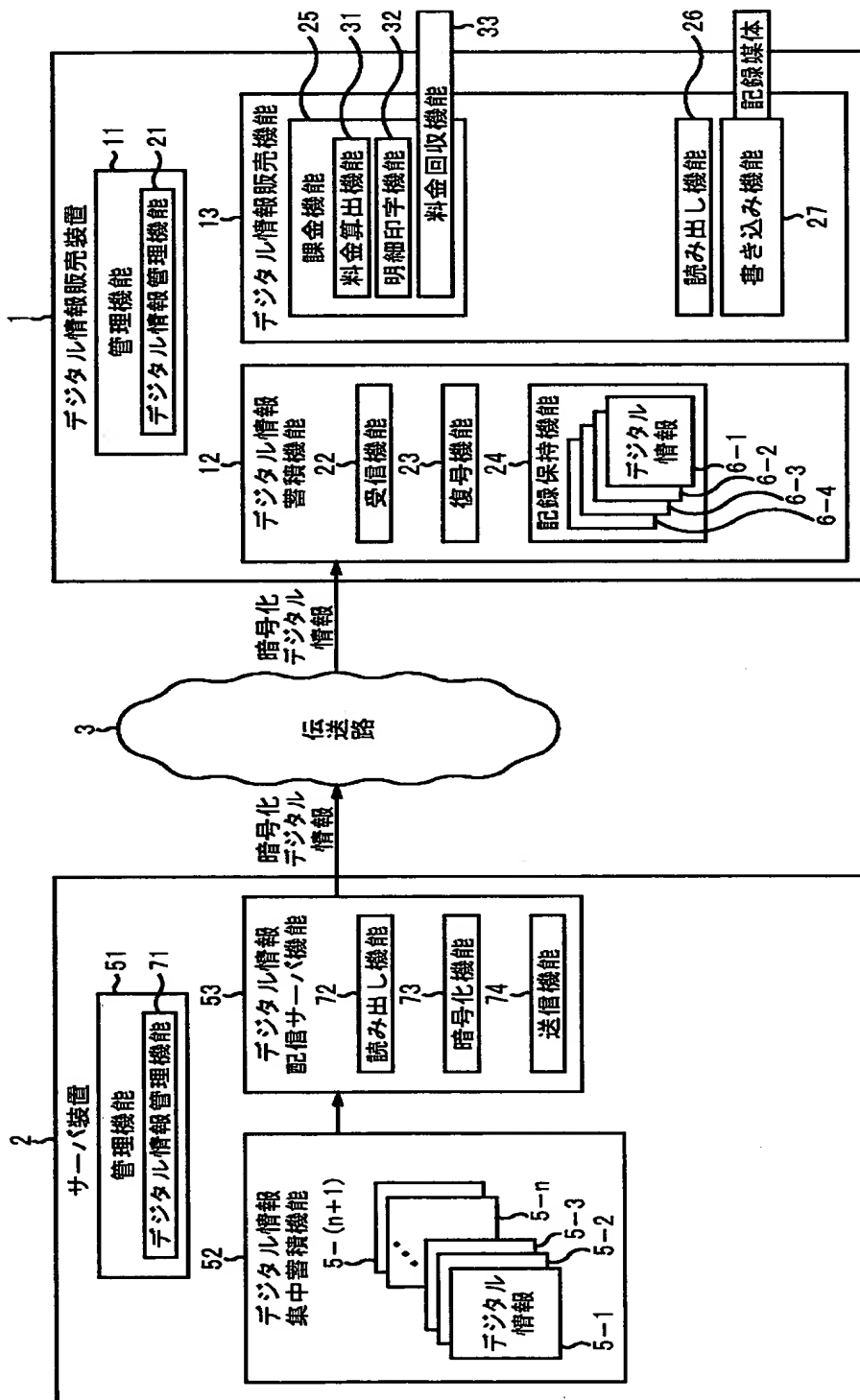
デジタル情報販売装置 101 のデジタル情報 6 の販売の他の処理を説明するフローチャートである。

【符号の説明】

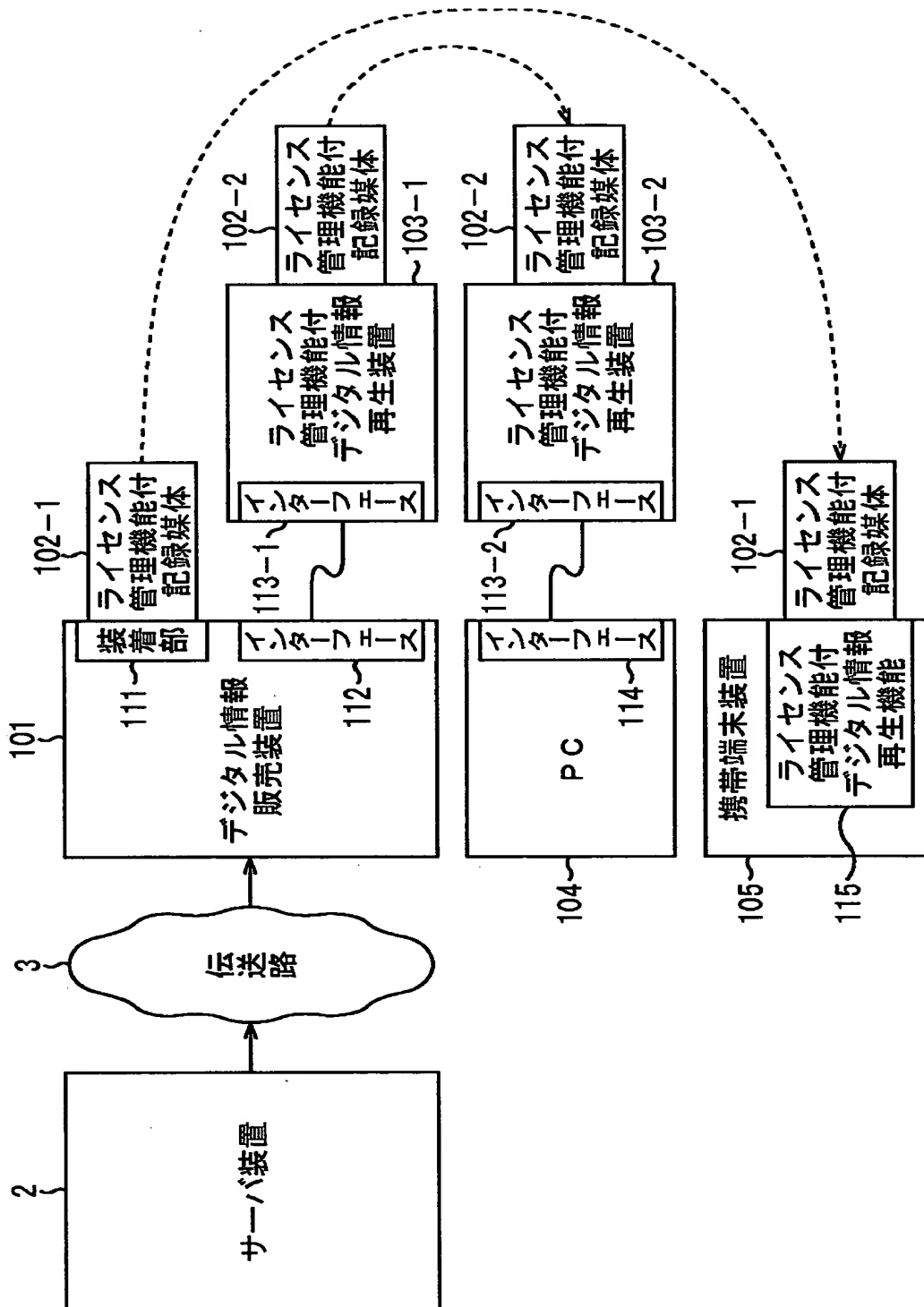
101 デジタル情報販売装置, 102-1, 102-2 ライセンス管理機能付記録媒体, 103-1, 103-2 ライセンス管理機能付デジタル情報再生装置, 112 インターフェース, 121 CPU, 122 ROM, 123 RAM, 128 通信部, 129 記録部, 131 書き込み部, 132 料金回収部, 161 磁気ディスク, 162 光ディスク, 163 光磁気ディスク, 164 半導体メモリ, 211 管理機能, 212 デジタル情報蓄積機能, 213 デジタル情報販売機能, 214 認証機能, 227 ライセンス生成機能, 228 デジタル情報鍵生成機能, 229 暗号化機能, 230 ライセンス付デジタル情報書き込み機能

【書類名】 図面

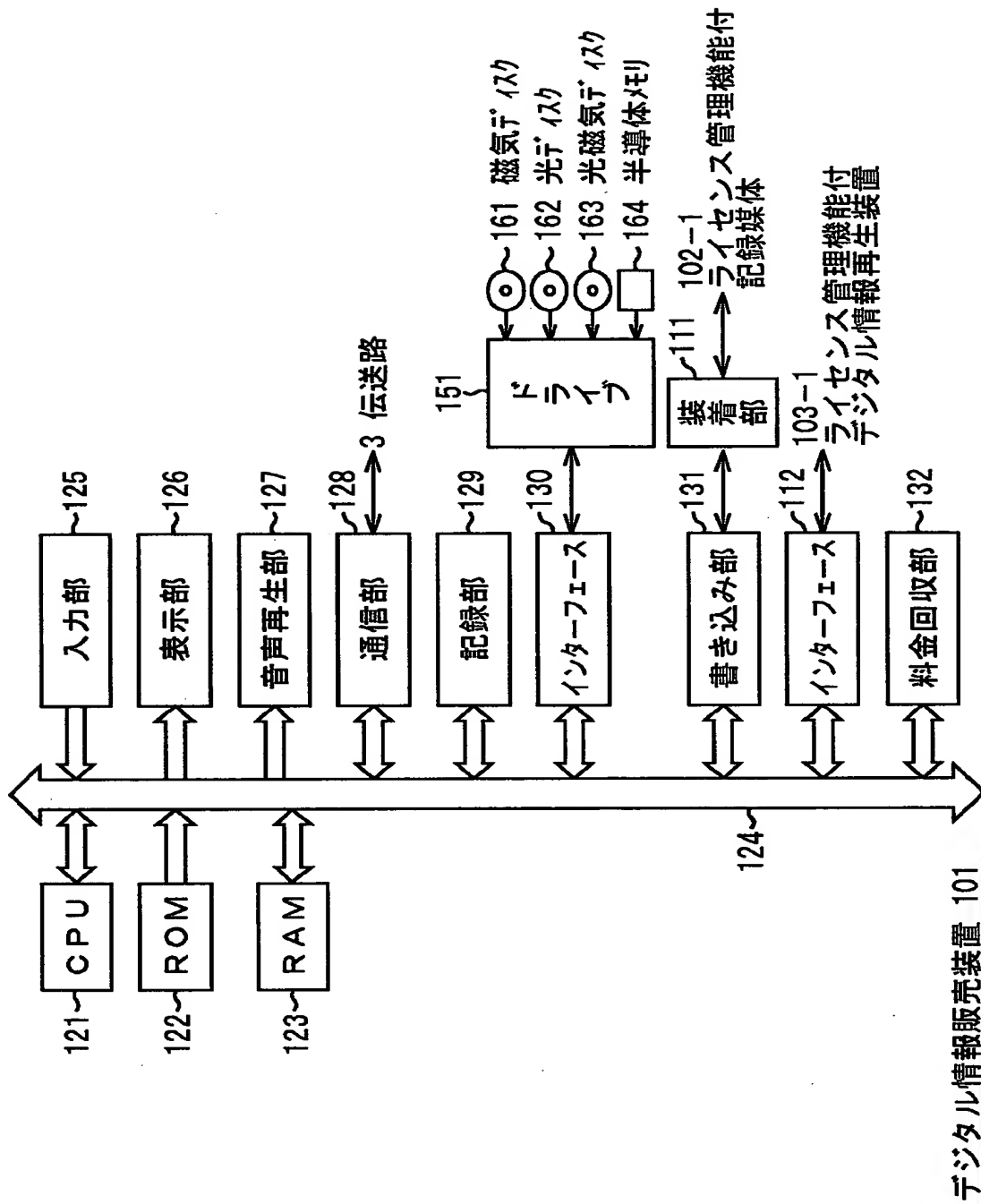
【図 1】



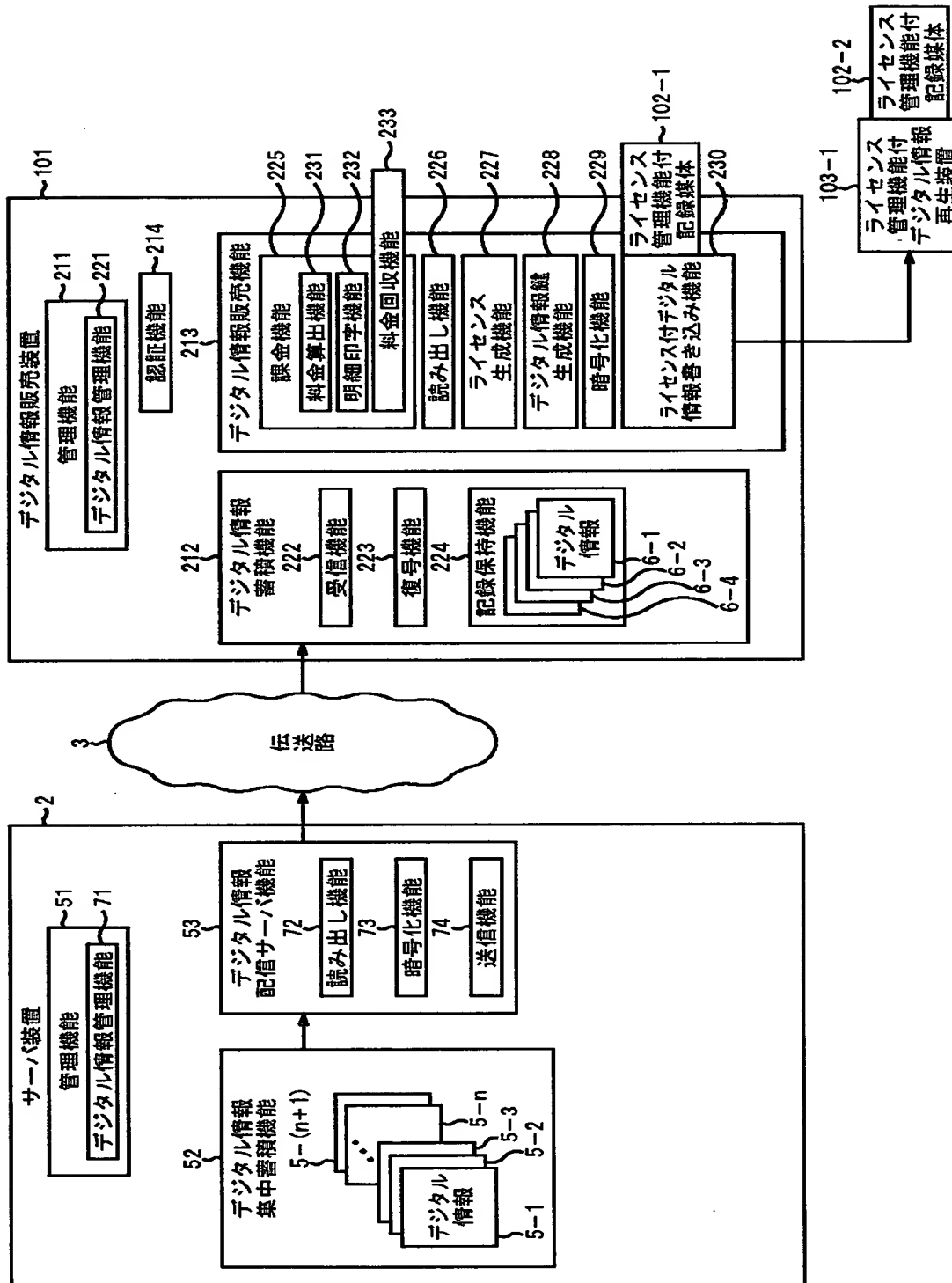
【図2】



【図 3】



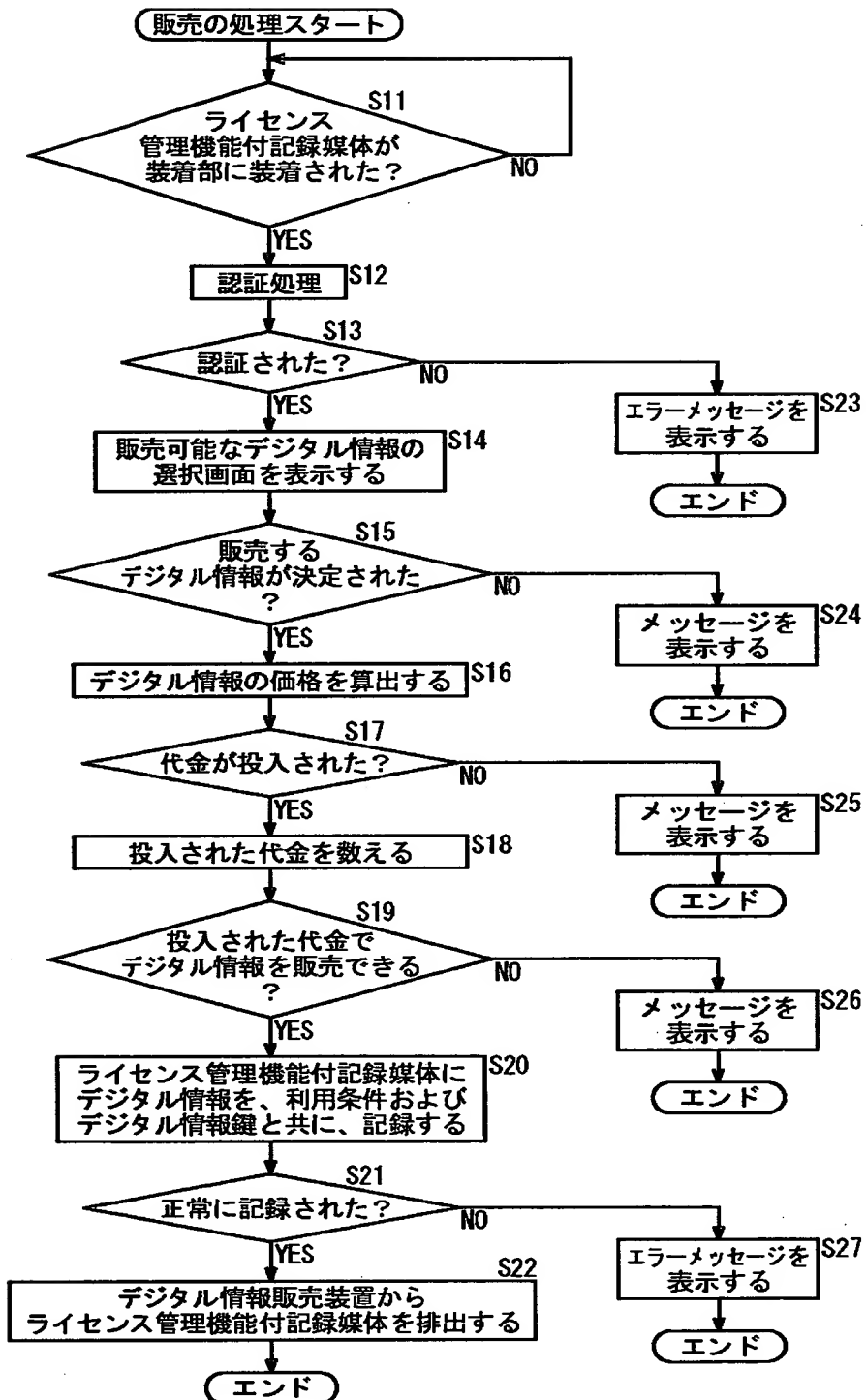
【図 4】



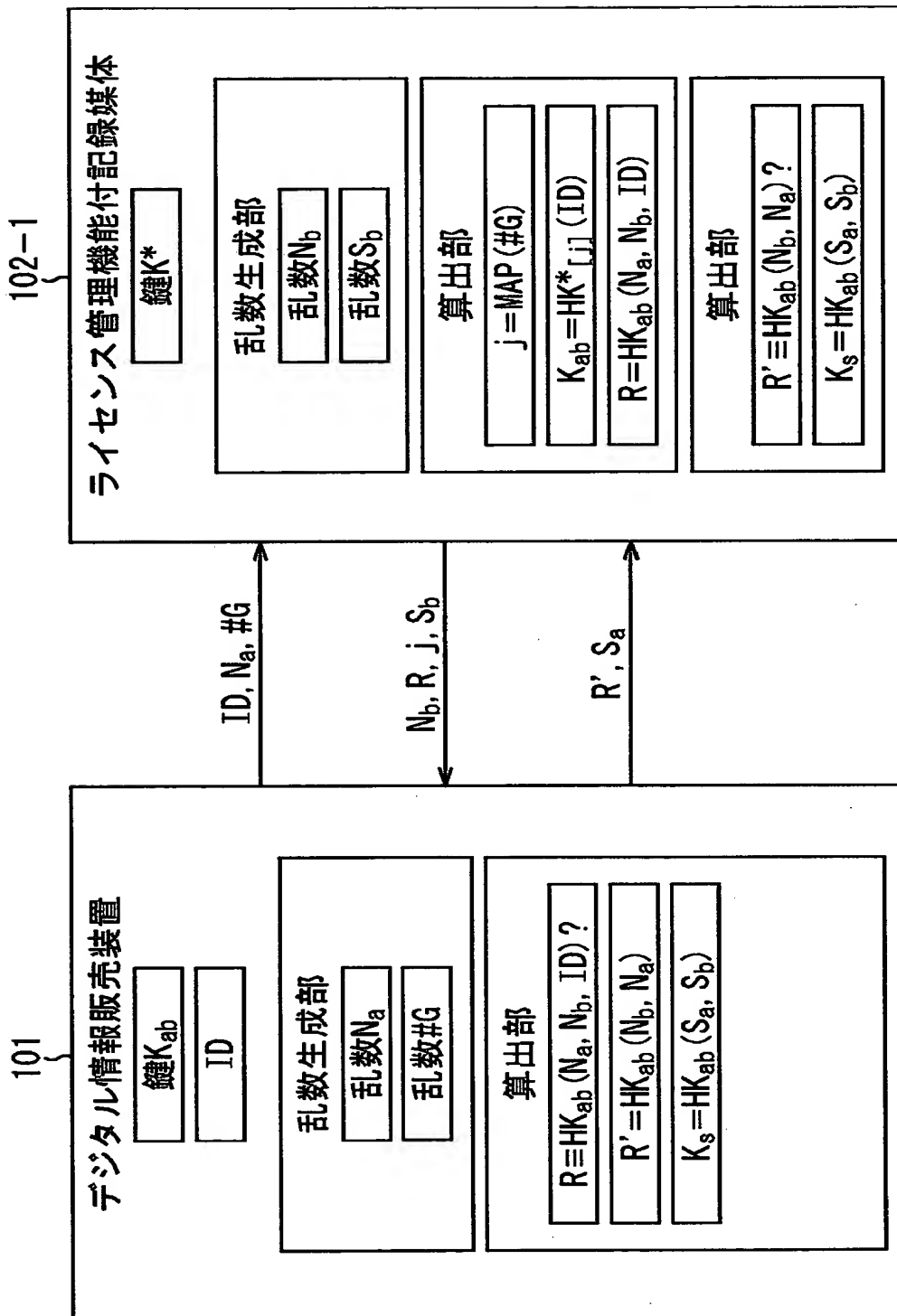
【図 5】

デジタル情報
利用条件
デジタル情報鍵

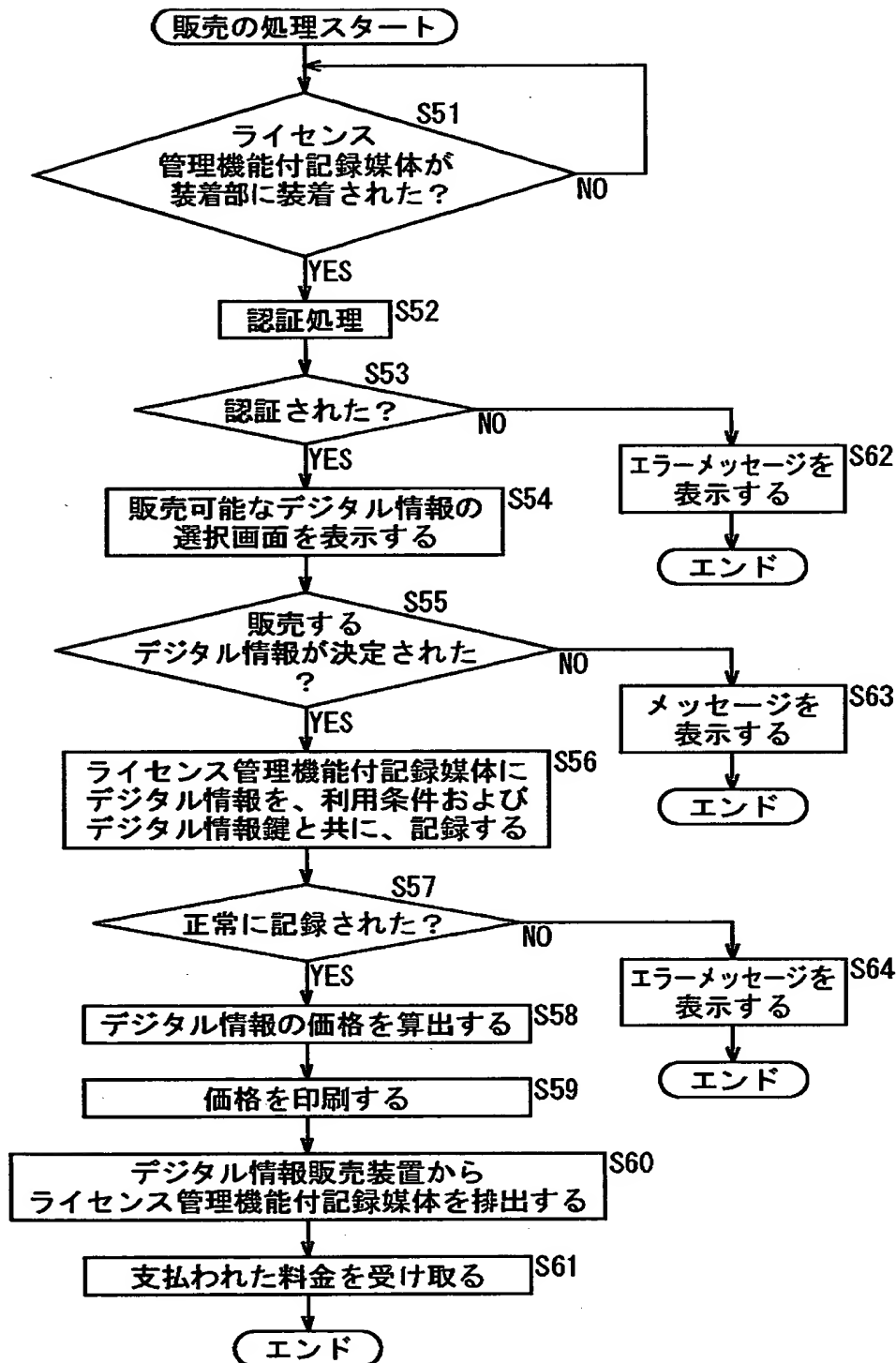
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 販売した情報の不正な利用を防止する。

【解決手段】 デジタル情報蓄積機能 2 1 2 は、販売するデジタル情報 6 を蓄積する。ライセンス生成機能 2 2 7 は、デジタル情報 6 に対応する利用条件を生成する。暗号化機能 2 2 9 は、デジタル情報 6 を暗号化する。デジタル情報鍵生成機能 2 2 8 は、暗号化されたデジタル情報 6 を復号する暗号鍵を生成する。認証機能 2 1 4 は、デジタル情報販売装置 1 0 1 に装着されているライセンス管理機能付記録媒体 1 0 2 - 1 を認証する。ライセンス付デジタル情報書き込み機能 2 3 0 は、認証されたライセンス管理機能付記録媒体 1 0 2 - 1 に、暗号化されたデジタル情報 6 を利用条件および暗号鍵と共に書き込む。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社